

REMARKS

Claims 1, 3, and 9 stand rejected as anticipated by Marvit. Claims 2, 4-8, and 10-28 stand rejected as obvious over Marvit in view of Stalling, Newton, or Stalling and Newton. Applicants respectfully traverse these rejections and beg for reconsideration in view of the remarks that follow.

In order to more distinctly and particularly claim that which they regard as their invention, applicants have cancelled claims 1-28, and have added new independent claims 29 and 30. As amended, the claims describe a method for authenticating a mobile terminal to a network. Specifically, the mobile terminal transacts with two different wireless communication networks, which are respectively referred to as "network A" and "network B" in the claims.

In typical applications of the present invention, network A has the capability to distribute an encryption key to the mobile station, but network B has no such capability. However, network B needs a secure way to distribute an authentication key (referred to in the claims as "SSD") to the mobile station, so that the mobile station can then use SSD to generate an authentication message that will gain it access to network B. All information which reaches the mobile station must be transmitted over the air.

The invention of newly presented claims 29 and 30 solves the problem faced by network B: It uses network A for secure key distribution. Specifically, network A distributes an encryption key to the mobile station. Network B generates SSD and delivers it to network A in some secure fashion, which will typically be over a wireline connection. Network A then uses the encryption key to securely transmit SSD to the mobile station. The mobile station uses SSD to generate an authentication message. The mobile station does not yet communicate directly with network B. Therefore, the mobile station passes the authentication message to network A for forwarding to network B. When network B receives and verifies the authentication message, it establishes direct communication with the mobile station.

New claim 29 claims the pertinent portion of the above-described process from the point of view of the mobile station. New claim 30 claims that portion which is pertinent from the point of view of network A.

All of the steps recited in claims 29 and 30 are included in the process outlined at Specification, page 4, line 6, to page 5, line 8. Accordingly, no new matter is introduced by the newly added claims.

Applicants submit that Marvik fails to teach, or even to suggest, any arrangement in which one wireless network distributes an encryption key for the benefit of a further wireless network. Much less, then, does Marvik suggest any arrangement in which the network which distributed the encryption key is then used to securely deliver to the mobile station an SSD generated by the further network. Much less still, does Marvik suggest any arrangement in which the network which distributed the encryption key is used to intercept an authentication message from the mobile station and forward it to the further network.

The secondary references which have been cited do not provide any of the teachings or suggestions which Applicants have pointed out as missing from Marvik. Accordingly, Applicants respectfully submit that the invention of new claims 29 and 30 is patentable over the cited references under the standards of 35 USC 102 and 103.

Having responded to all points of rejection, Applicants respectfully solicit allowance of claims 29 and 30.

Respectfully,



Martin I. Finston, Attorney
Reg. No. 31613
908-582-2908

Date: July 8, 2004
Docket Administrator (Room 3J-219)
Lucent Technologies Inc.
101 Crawfords Corner Road
Holmdel, NJ 07733-3030